DHMH Architecture and Standards

Table of Contents

Introduction:

The purpose of Architecture and Standards is to achieve interconnectivity and interoperability between heterogeneous systems. Said differently, architectures and standards allow dissimilar systems to share resources such as communications facilities, databases and applications.

Standards are important. They are analogous to "rules of the road". For example, for auto traffic, they describe the protocols or procedures by which autos can interact with each other (e.g., who has the "right-of-way) and avoid a collision. What is most important is that there is a standard; frequently, which standard is chosen is of little importance. The purpose of this document is to describe the way in which DHMH users can most efficiently and effectively share resources within DHMH. Thus, it describes the strategic direction of IT within DHMH.

Standards have always been important in IT. They define how hardware and software and telecommunications components will operate with one another. However, their importance has changed dramatically in recent years. Historically, vendors such as IBM, HP and Digital defined their architecture and standards and developed products to conform to the standards. With the arrival of distributed computing and heterogeneous (dissimilar) systems, the burden of defining an architecture and standards has moved to user organizations. Each organization must develop their own.

What This Document Is:

The purpose of this document is to provide guidance to DHMH users (and other interested parties) about the strategic direction of IT within DHMH and how best to use that strategic blueprint to your advantage. It is important to DHMH users that are planning and/or developing new systems and/or major modifications to existing systems that will share resources within DHMH. It describes the "rules of the road" for interconnecting and/or interoperating with other DHMH users and resources.

Architecture and Standards are important if you share resources with other DHMH users. Shared resources include hardware, software, middleware, data and perhaps most importantly, people and skills (e.g., IRMA support). Standalone systems are not affected.

In addition, architecture and standards are presented as *guidance* to users. Users are free to make their own architecture and standards and product decisions. However, this "blueprint" is the strategic direction of DHMH. Users that choose to go their own way must recognize that they risk creating an "island of automation", with little or no support, and will be "on their own". The quantity and quality of IRMA support will increase over time for architecturally compliant systems and will be limited (at best) and diminish over time for architecturally non-compliant systems. We expect most Agencies will choose to align with the architecture and standards described in this document for their own self-interest.

You should view this document as a "work in process". Standards are a moving target. We believe these standards represent the best available choices today .i.e., we believe they represent the "common good". Nevertheless, all standards evolve and change over time and new ones emerge. In addition, The relative strengths of vendor products and services to address these standards changes over time as well. We have described each standard and its expected evolution over time (next 3 years). In each case, we believe the standard chosen is the best available solution today. This document will be updated periodically (at least yearly) to reflect the evolution of the standards and the relative strengths of vendor solutions.

Users have a choice. Different standards and/or vendor products and services may be better for a particular application. This could happen for many reasons most frequently due to the adoption of a software package that incorporates different standards or a decision to use a 3rd party that has adopted different standards. There are strategies that can minimize the differences between DHMH standards and your application. For example, we strongly recommend that you adopt high-level interfaces that allow you to interconnect and interoperate with the DHMH standards. We also strongly recommend that you have a strategy for moving closer to the DHMH standards over time. We will help you to develop these strategies.

Who is Affected:

Architecture and Standards described in this document primarily apply to DHMH users. They may be important to other users that need to interconnect and/or interoperate with DHMH. To the maximum extent possible, these standards are consistent with the standards of external organizations with whom we interact such as DBM, US Government and others. We have cross-referenced other applicable standards in the Appendix.

Why is this Document Important?

This document describes DHMH's IT investment strategy. DHMH will spend approximately $30 M per year for IT in each of the next several years. That money will be used to purchase hardware, software and telecommunications services, develop applications, build infrastructure and develop skills and support organizations. This document is the blueprint for how that money will be spent. Thus, it is the mainstream direction of where DHMH intends to go and what it will acquire, build and deploy.

Perhaps most importantly, it describes what resources will be developed which directly affects the quantity and quality of resources available to users. The resources most affected are:

Tech Support - We will invest in people and skills through hiring, training and work experience to develop these skills

Help Desk - We will invest in organizations and support services that can assist you with these standards

Standard Interfaces - We will buy hardware, software, middleware and telecommunications products and services that meet these standards

Operations - We will invest in processes that support delivery within these standards

We expect that levels of service and support, as well as the costs of support, will be significantly different between architecturally compliant systems and those that are not architecturally compliant. Said differently, there will be more and better support, at lower cost, to architecturally compliant users. In addition, there will be a "snowball effect" i.e., this gap will widen over time. As more and more users and DHMH systems and resources adopt these standards, interconnection and interoperation for non-compliant systems will become increasingly difficult.

How to Use This Document:

This document is provided as guidance. It shows DHMH's strategic intent, i.e., the direction in which the "ship" will go. We believe it is in the best interests of users to align with this strategic direction.

We strongly recommend that you adopt these standards as soon as possible. Nevertheless, we recognize that it is not always possible to align with a strategic direction immediately. If you can do it now, we strongly urge you to do so. If you cannot, we strongly recommend that you develop strategies (such as high-level interfaces and/or minimizing the use of proprietary features) that will facilitate your adopting the standards in the future. We strongly recommend that you develop a plan for aligning with these standards in the future. We will help you do this.

If you choose to adopt a different standard, you are responsible for interfacing with the DHMH standard. You must acquire, integrate and deploy the products and services - and the skills - that allow interconnection and interoperation with DHMH systems.

The risk in following a different architectural or standards path is that you become an "island of automation" that cannot interconnect and/or interoperate with other DHMH organizations and systems. As time passes and more and more users align with these standards, the differences and difficulties will increase. So too, the quantity and quality of support will diminish and the cost of support will increase.

For guidance regarding the most current hardware and software configurations, supporting products and vendors, please contact the Help Desk.

Benefits to Users:

The benefit to users of adopting this architecture and standards are simple but very important. Users will get their applications up and running faster, cheaper, with less risk and with a higher probability of success. Said differently, users can leverage the resources of DHMH by adopting this blueprint rather than "going it alone". This is true for new development as well as in production operations.

Standards

Client Access Control	
DBMS	
Encryption	
Host Access Control	
Project Management	
Server Operating System	
Server Hardware	

Client Access Control Standard

1. What does the Standard do? -- A client-based security service that presents a client identity to the host for access to the IRMA network and network resources.

   - Smart Card
   - Token
   - Digital Certificate
   - Biometrics

2. Why is this Standard Needed?

   It identifies a client for network and application access within DHMH. This standard is mandated by HIPPA legislative requirements. It also complies with DHMH and State Data Security policies.

3. Who are the principal stakeholders that are concerned with this standard?

   All DHMH Agencies that share resources with other DHMH organizations. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems.

4. Which vendors make products that support the standard

   - Smart Card — No Preference
   - Token — Secure ID
   - Digital Certificate — Novell
   - Biometrics — No Preference

5. How will the standard evolve?

   - This year — Token, Smart Cards
   - In one to two years — Digital Certificates, Token, Smart Cards
   - Three years and beyond — Biometrics, Smart Cards

DBMS Standard

6. What does the Standard do? -- Defines a data architecture for organizing and managing data.

    - ACCESS
    - Oracle
    - Microsoft SQL
    - MYSQL

7. Why is this Standard Needed?

    It standardizes data formats to facilitate data sharing within DHMH. It also provides data security, enables trans-firewall communication and provides economies of scale (software licensing, applications support and maintenance and training).This standard is mandated by HIPPA, Medical Records and Privacy Act legislative requirements. It complies with State Data Security policy.

8. Who are the principal stakeholders that are concerned with this standard?

    All DHMH Agencies that share data. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems. In addition, External Trusted Business Partners that interconnect and/or interoperate with DHMH are affected.

9. Which vendors make products that support the standard

• ACCESS	Microsoft
• Oracle	Oracle
• Microsoft SQL	Microsoft
• MYSQL	Redhat (Linux)

10. How will the standard evolve?

    The most current -- and most stable -- production release should be used with all service upgrades installed. Beta versions should not be used for production applications.

Encryption Standard

11. What does the Standard do? -- The standard defines an algorithm and a process, based on a predetermined set of keys, for encoding information that can only be decoded by authorized persons. There are many forms of encryption available including symmetric, asymmetric, proprietary and Public Key Infrastructure (PKI). PKI, as implemented by Novell, is the strategic direction for DHMH and the State. The standard can be implemented by:

    - 3DES
    - AES
    - SSL-3 (Secure Socket Layer 3)
    - VPN

12. Why is a Standard Needed?

    This standard protects information from alteration and theft and maintains confidentiality, integrity and availability. It is mandated by HIPPA legislation. It meets DHMH and State Data Security policies.

13. Who are the principal stakeholders that are concerned with this standard?

    All DHMH Agencies that share resources with other DHMH organizations. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems.

14. Which vendors make products that support the standard

    - 3DES — Novell
    - AES — Novell
    - SSL-3 — Netscape, Internet Explorer (V5 or later)
    - VPN — IPSEC V3

15. How will the standard evolve?

    - This year — 3DES, SSL-3, VPN
    - In one to two years — AES, SSL-3, VPN
    - Three years and beyond

16. Avoid password-based encryption methods.

Host Access Control Standard

17. What does the Standard do? -- A network-based security service that ensures you are who you say you are. It prevents unauthorized access to the network and network resources.

    - LDAP (X.509)
    - Radius Access Server / Client ID
    - Digital Certificates (DHMH or 3rd Party Issuer)
    - VPN

18. Why is this Standard Needed?

    It simplifies and controls network and application access within DHMH. This standard is mandated by HIPPA legislative requirements. It also complies with State Data Security policy.

19. Who are the principal stakeholders that are concerned with this standard?

    All DHMH Agencies that share resources with other DHMH organizations. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems. In addition, External Trusted Business Partners that interconnect and/or interoperate with DHMH are affected.

20. Which vendors make products that support the standard

    - LDAP (X.509) Novell
    - Radius Access Server / Client ID Secure ID
    - Digital Certificates Novell
    - VPN Gauntlet

21. How will the standard evolve?

    - This year Tokens
    - In one to two years Digital Certificates
    - Three years and beyond

Project Management Standard

22. What does the Standard do? -- It defines a structured approach to Applications Development including technical, logistical, material and personnel resources needed.

    The DHMH strategic direction is to adopt Capability Maturity Model Level 2 (CMM-2).

23. Why is this Standard Needed?

    It assures that projects are defined, documented and deliver their intended results. It also serves as the basis for agreement between parties to the effort. All projects require some form of project management. Large projects (e.g., projects with high visibility or certain funding sponsors or involving multiple Agencies or costing over $500,000 or with high levels of complexity or over one year duration) require CMM-2 level project management. It complies with DHMH and IT and Procurement policies.

24. Who are the principal stakeholders that are concerned with this standard?

    DBM, DHMH and Agency senior management and system owners. In addition, funding sources such as Maryland Legislature, HCFA and others are concerned. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems.

25. Which vendors make products that support the standard?

    Any project management product or service that is CMM-2 certified.

26. How will the standard evolve?

    None expected.

Server Hardware Standard

27. What does the Standard do?

    This standard defines a server configuration that can be supported by IRMA to meet availability requirements (i.e. it eliminates single points of failure) and physical space limitations.

    The hardware configuration must be rack-mounted (physical constraint) and have redundant a) power supplies on two independently fused circuits, b) NICs and c) RAID (availability requirement).

28. Why is a Standard Needed?

    Agencies that wish to obtain operations support and/or locate their hardware in IRMA facilities must meet these physical requirements. The standards meet US Critical Infrastructure Assurance Office (CIAO) standards and best practices.

29. Who are the principal stakeholders that are concerned with this standard?

    All DHMH Agencies that share resources with other DHMH organizations. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems.

30. Which vendors make products that support the standard

    Compaq, Dell Computer Corporation

31. How will the standard evolve?

    - This year
    - In one to two years
    - Three years and beyond

Server Operating System Standard

32. What does the Standard do?

    The standard defines a server environment that can be supported by IRMA. This environment comprises NT for the Application Operating System (AOS) and Novell for the Network Operating System (NOS).

33. Why is a Standard Needed?

    NOS is required for interoperability between DHMH Agencies. In addition, Agencies that wish to obtain support (including operations, tech support, training and/or Help Desk) from IRMA must meet this standard.

34. Who are the principal stakeholders that are concerned with this standard?

    All DHMH Agencies that share resources with other DHMH organizations. Agencies most affected are those planning and/or developing new systems or major modifications to existing systems.

35. Which vendors make products that support the standard

    Microsoft, Novell

36. How will the standard evolve?

- This year — NT with all service packages
- In one to two years — Windows 2000 with all service packages
- Three years and beyond — Microsoft

Appendices

Cross References

DHMH must meet standards originating from many other organizations. This document defines DHMH-specific standards. For your convenience, we include a cross-reference to other standards with which we must comply and/or be aware of. At a minimum, they provide guidance as to best practices.

Topic	Source	HTML Reference
Hardware Standards and Technology Refresh	DBM #1	
Software Standards (COTS)	DBM #2	
Data Security	DBM #3	
IT Architecture	DBM #4	
Network Design and Operation	DBM #5	
E-Mail and Internet Use	DBM #6	
Web Site Development and Operations	DBM #7	
Universal Privacy	DBM #8	
Project Management	DBM #10	
Contract Management	DBM #11	
Configuration Management	DBM #12	
Universal Electronic Accessibility	DBM #13A	
Teleworking	DBM #13B	
Systems Development	DBM #16	
Hardware and Infrastructure Financing	DBM #17	
Training and Certification	DBM #20	
Capacity Planning	DBM #21	
Cost Effective IT Management	DBM #22	
Hardware and Software Inventory Procedures	DBM #23	
Vulnerability Assessment	CIAO	

Definitions:

1. LDAP -- A directory database of individual identifiers. X.509 is the NIST standard for LDAP that describes interoperable directory information.

2. PKI --

3. SSL-3 -- Secure Socket Layer 3. A 128 bit encryption process within a browser such as Netscape or Internet Explorer (V5 or later)

4. VPN -- Virtual Private Network

5. Smart Card-- A carrier (usually credit card size) containing memory and a microprocessor used in conjunction with a Smart Card reader for identification.

6. Token -- A pager-size active carrier containing a random number generator that is synchronized to a server for identification

7. Digital Certificate -- A set of electronic information that uniquely identifies an individual for access control and generation of encryption codes

8. 3rd Part Digital Certificate -- A Digital Certificate, issued by an independent 3rd party, to maintain control

9. AES --

10. 3DES --

11. Middleware -- Software that links dissimilar systems and allows them to interconnect and/or interoperate

12. Digital Signature --